Kuptimi I mbrojtjes

Mbrojtja e thellë
Asetet, Rreziqet, Kërcënimet

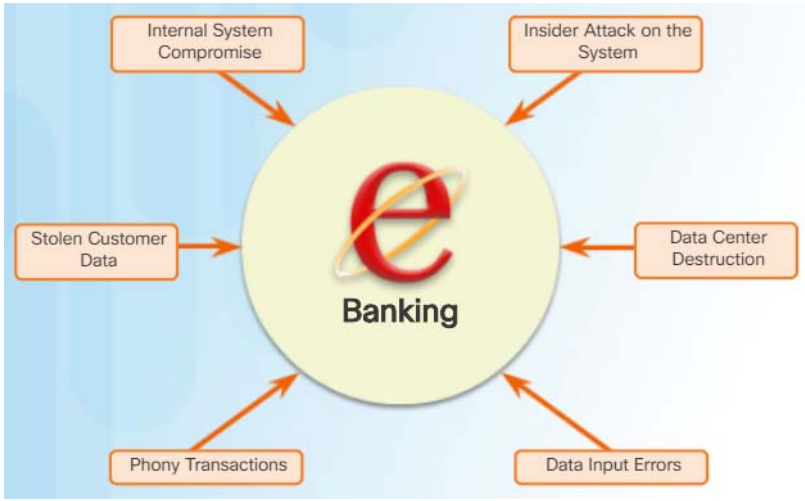
- Rreziku i sigurisë kibernetike përbëhet nga:
  - Asete - Çdo vlerë e një organizate që duhet të mbrohet, duke përfshirë serverat, pajisjet infrastrukturore, pajisjet përfundimtare dhe asetet më të mëdha, të dhënat.
  - Rreziqet - Një dobësi në një sistem apo dizajnin e tij që mund të shfrytëzohet nga një kërcënim.
  - Kërcënimet - Çdo rrezik potencial për një aset.

Mbrojtja e thellë
Identifikimi I Aseteve

- Shumë organizata kanë vetëm një ide të përgjithshme të aseteve që duhet të mbrohen.
- Të gjitha pajisjet dhe informatat në pronësi ose të menaxhuara nga organizata janë pasuritë.
- Asetet përbëjnë sipërfaqen e sulmit që kërcënojnë aktorët mund të synojnë.
- Menaxhimi i pasurisë përbëhet nga:
  - Inventarizimi i të gjitha aseteve.
  - Zhvillimi dhe zbatimi i politikave dhe procedurave për mbrojtjen e tyre.
- Identifikoni se ku ruhen asetet kritike të informacionit dhe se si fitohet aksesi për këtë informacion.

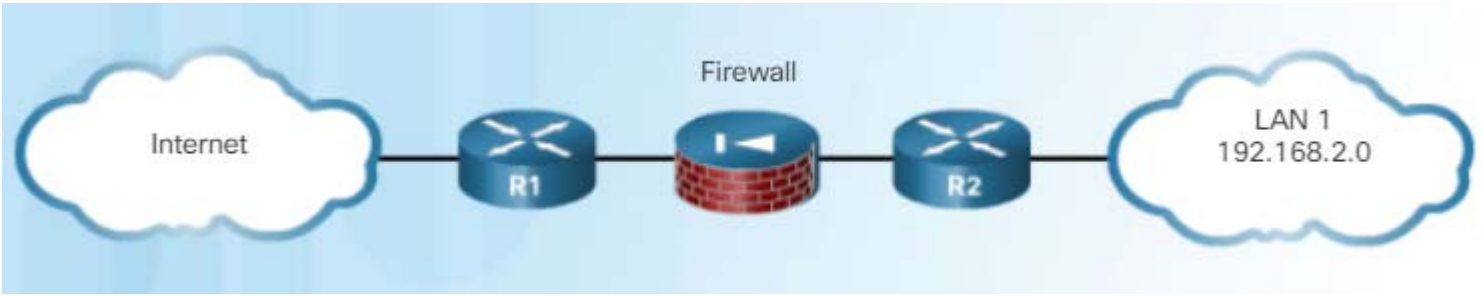
Mbrojtja e thellë
Identifikimi i cenueshmërisë

- Identifikimi i dobësive përfshin përgjigjet në pyetjet e mëposhtme:
  - Cilat janë dobësitë?
  - Kush mund të shfrytëzojë dobësitë?
  - Cilat janë pasojat nëse dobësia është shfrytëzuar?
- Për shembull, një sistem e-banking mund të ketë kërcënimet e mëposhtme:
  - Kompromis i sistemit të brendshëm
  - Të dhënat e vjedhura të konsumatorëve
  - Transaksionet e rreme
  - Sulmi i brendshëm në sistem
  - Gabimet e futjes së të dhënave
  - Shkatërrimi i qendrës së të dhënave



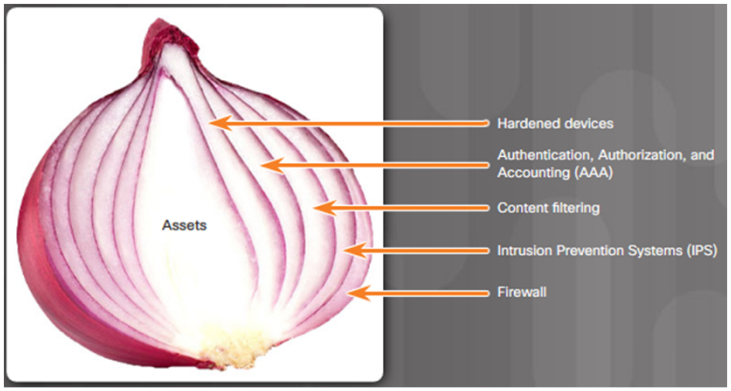
Mbrojtja e thellë
Identifikimi i Kërcënimeve

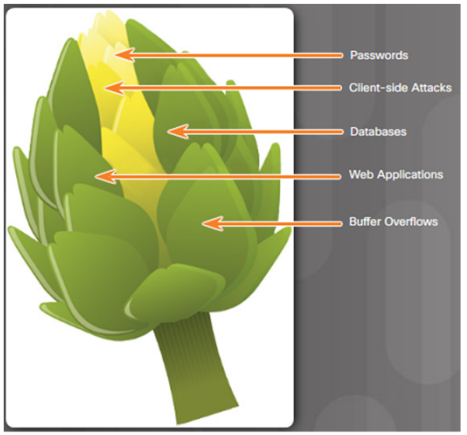
- Përdorimi i një qasjeje të mbrojtjes në thellësi për të identifikuar asetet mund të përfshijë një topologji me pajisjet e mëposhtme:
  - Router Edge - rreshtin e parë të mbrojtjes; konfiguruar me një sërë rregullash që përcaktojnë se cili trafik lejon ose mohon.
  - Firewall - Një linjë e dytë e mbrojtjes; kryen filtrim shtesë, autentifikim të përdoruesit dhe gjurmon gjendjen e lidhjeve.
  - Router i brendshëm - një linjë e tretë e mbrojtjes; zbaton rregullat përfundimtare të filtrimit në trafik para se të përcillet në destinacionin e tij.



Mbrojtja e thellë
Qepja e Sigurisë dhe Qasjet e Artichokës së Sigurisë

- Analogjia e qepëve të sigurisë ilustron një qasje të shtresuar ndaj sigurisë.
- Një aktor kërcënues do të duhet të heqë larg mekanizmave mbrojtës të rrjetit një shtresë në të njëjtën kohë.
- Megjithatë, me evoluimin e rrjeteve pa kufij, një artichoke sigurie është një analogji më e mirë.
- Akterët e kërcënimeve mund të kenë nevojë vetëm për të hequr disa "gjethe angjie" për të hyrë në të dhëna të ndjeshme.
- Për shembull, një pajisje celulare është një fletë që, kur kompromentohet, mund t'i japë aksesit të kërcënuesit qasje në informacione të ndjeshme siç janë email-i i korporatës.
- Dallimi kryesor midis qepës së sigurisë dhe artikut të sigurisë është se jo çdo fletë duhet të hiqet për të marrë në të dhënat.



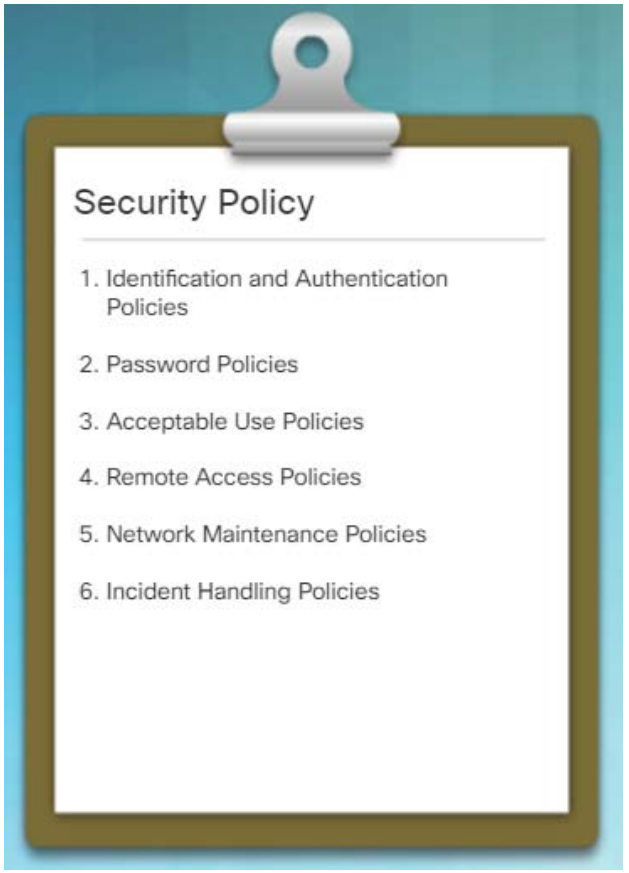


Politikat e Sigurisë
Politika e Biznesit

- Politikat sigurojnë themelin për sigurinë e rrjetit duke përcaktuar atë që është e pranueshme.
- Politikat e biznesit janë udhëzimet e zhvilluara nga një organizatë që qeverisin veprimet e saj dhe veprimet e punonjësve të saj.
- Një organizatë mund të ketë disa politika udhëzuese:
  - Politikat e kompanisë - vendosin rregullat e sjelljes dhe përgjegjësitë e punonjësve dhe punëdhënësve.
  - Politikat e punonjësve - identifikoni pagën e punonjësve, orarin e pagesës, përfitimet e punonjësve, orarin e punës, pushimet, dhe më shumë.
  - Politikat e sigurisë - identifikojnë një sërë objektivash të sigurisë për një kompani, përcaktojnë rregullat e sjelljes për përdoruesit dhe administratorët dhe përcaktojnë kërkesat e sistemit.

Politikat e Sigurisë

- Një politikë gjithëpërfshirëse e sigurisë ka një numër përfitimesh:
  - Demonstron angazhimin e një organizate për sigurinë.
  - Vendos rregullat për sjelljen e pritshme.
  - Siguron qëndrueshmëri në operacionet e sistemit, blerjen dhe përdorimin e softuerëve dhe pajisjeve dhe mirëmbajtjen.
  - Përcakton pasojat ligjore të shkeljeve.
  - I jep personelit të sigurisë mbështetjen e menaxhmentit.
- Një politikë sigurie mund të përfshijë një ose më shumë nga artikujt e treguar në figurë.
- Një politikë e përdorimit të pranueshëm (AUP) është një nga politikat më të zakonshme dhe mbulon atë që përdoruesit janë të lejuar dhe nuk lejohen të bëjnë në komponentët e ndryshëm të sistemit.



Politikat e Sigurisë
Politikat BYOD

- Shumë organizata mbështesin Sjelljen e Pajisjes Tuaj (BYOD), i cili u mundëson punonjësve të përdorin pajisjet e tyre mobile për të pasur qasje në burimet e kompanisë.
- Një politikë BYOD duhet të përfshijë:
  - Specifikoni qëllimet e programit BYOD.
  - Identifikoni cilat punonjës mund të sjellin pajisjet e tyre.
  - Identifikoni se cilat pajisje do të mbështeten.
  - Identifikoni nivelin e aksesit të punonjësve që jepen gjatë përdorimit të pajisjeve personale.
  - Përshkruani të drejtat për qasje dhe aktivitetet e lejuara për personelin e sigurisë në pajisjen.
  - Identifikoni cilat rregulla duhet të respektohen kur përdoren pajisjet e punonjësve.
  - Identifikoni masat mbrojtëse për të vendosur nëse një pajisje është kompromentuar.

Politikat e Sigurisë
Politikat BYOD (Vazh.)

- Praktikat më të mira të sigurisë të BYOD në vijim ndihmojnë në zbutjen e rreziqeve BYOD:
  - Qasja e mbrojtur me fjalëkalim për çdo pajisje dhe llogari.
  - Lidhja me valë e kontrolluar me dorë në mënyrë që pajisja lidhet vetëm me rrjetet e besueshme.
  - Mbani software përditësuar për të zbutur kundër kërcënimeve të fundit.
  - Rezervoni të dhënat në rast se pajisja humbet ose vjedh.
  - Aktivizo shërbimet e gjetjes "Gjej pajisjen time" që mund të fshijë një pajisje të humbur.
  - Sigurimi i softuerit antivirus.
  - Përdorni softuerin e Menaxhimit të Pajisjeve Mobile (MDM) për t'u mundësuar ekipeve të TI-së të zbatojnë parametrat e sigurisë dhe konfigurimet e softuerit në të gjitha pajisjet që lidhen me rrjetet e kompanisë.

Politikat e Sigurisë
Rregulloret dhe standardet e pajtueshmërisë

- Rregulloret dhe standardet e pajtueshmërisë përcaktojnë se cilat organizata janë përgjegjëse për ofrimin dhe përgjegjësinë nëse ato dështojnë të përmbushin.
- Rregullat e pajtueshmërisë që një organizatë është e detyruar të ndjekin varen nga lloji i organizatës dhe të dhënat që merret nga organizata.
- Rregullat specifike të pajtueshmërisë do të diskutohen më vonë gjatë kursit.

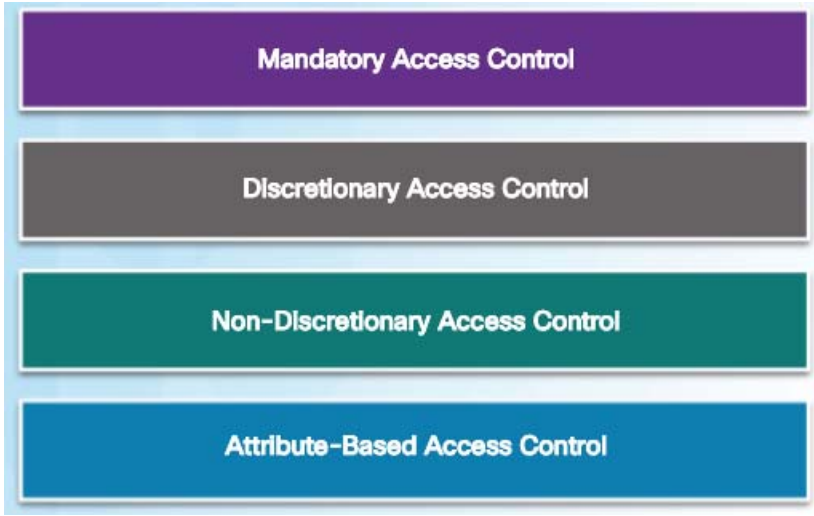
Kontrolli i Qasjes

Konceptet e Kontrollit të Qasjes
Siguria e Komunikimeve: CIA

- Siguria e informacionit merret me mbrojtjen e informacionit dhe sistemeve të informacionit nga aksesi, përdorimi, zbulimi, prishja, modifikimi ose shkatërrimi i paautorizuar.
- Treshja e CIA-s përbëhet nga:
  - Konfidencialiteti - vetëm njësitë e autorizuara mund të kenë qasje në informata.
  - Integriteti - informacioni duhet të mbrohet nga ndryshimet e paautorizuara.
  - Disponueshmëria - informacioni duhet të jetë në dispozicion të palëve të autorizuara që kërkojnë atë, kur e kërkojnë atë.

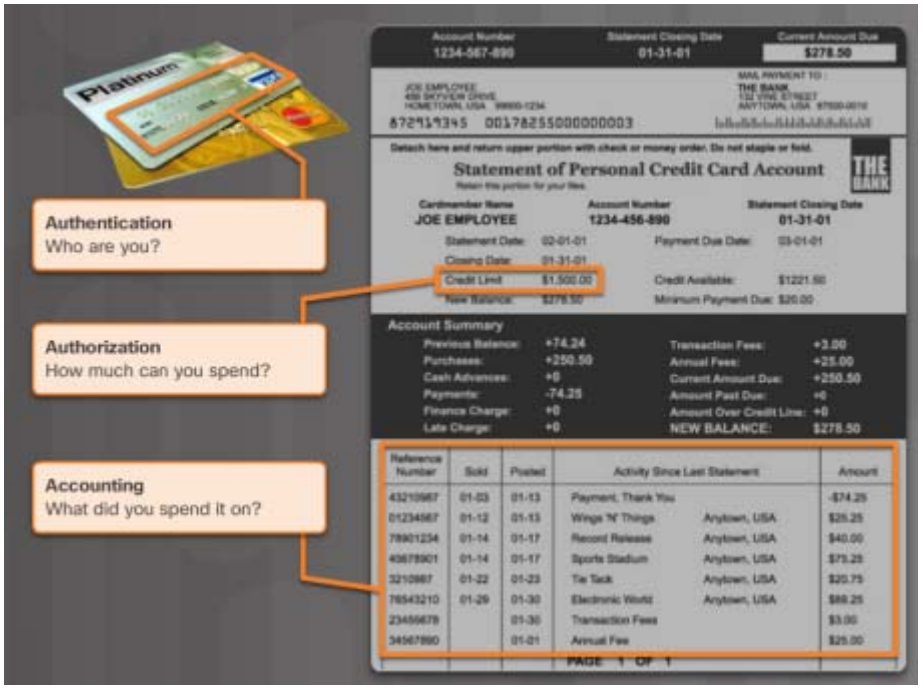
Konceptet e Kontrollit të Qasjes
Modelet e Kontrollit të Hyrjes

- Modelet e kontrollit të qasjes bazë përfshijnë si në vijim:
  - Kontrolli i detyrueshëm i qasjes (MAC) - zbaton kontrollin më të rreptë të qasjes, duke mundësuar aksesin e përdoruesit bazuar në pastrimin e sigurisë.
  - Kontrolli diskrecional i aksesit (DAC) - lejon përdoruesit të kontrollojnë qasjen në të dhënat e tyre si pronarë të atyre të dhënave.
  - Kontrolli jo-diskrecional i qasjes - qasja bazohet në role dhe përgjegjësi; i njohur gjithashtu si kontrolli i qasjes së bazuar në role (RBAC).
  - Atributi i bazuar në kontrollin e qasjes (ABAC) - qasja bazohet në atributet e burimit të qasur, përdoruesit që i qasen asaj dhe faktorëve të mjedisit, siç është koha e ditës.
- Një tjetër model i kontrollit të qasjes është parimi i privilegjit më të vogël, i cili thotë se përdoruesve duhet t'u jepet shuma minimale e aksesit që kërkohet për të kryer funksionin e tyre të punës.



Përdorimi i AAA

- Autentifikimi, Autorizimi dhe Kontabiliteti (AAA) është një sistem i shkallëzuar për kontrollin e qasjes.
  - Authentication - përdoruesit dhe administratorët duhet të provojnë se ata janë ata që thonë ata janë.
  - Autorizimi - përcakton cilat burime përdoruesi mund të hyjë dhe cilat operacione përdoruesi lejohet të kryejë.
  - Kontabiliteti - regjistron atë që përdoruesi e bën dhe kur e bëjnë atë.

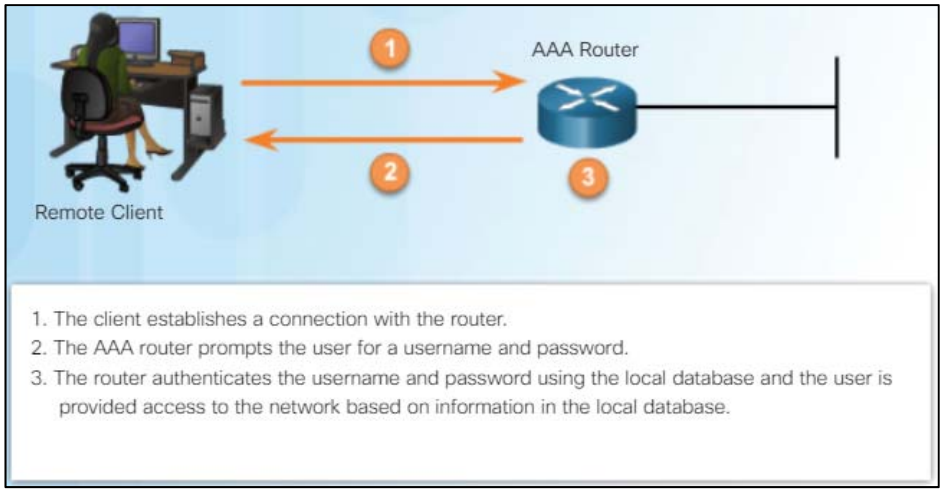


Përdorimi i AAA

- Dy metoda të zakonshme AAA të legalizuara përfshijnë:
  - Authentication AAA Local - Kjo metodë vërteton përdoruesit kundër përdoruesve dhe fjalëkalimeve të ruajtura në nivel lokal. AAA lokale është ideale për rrjetet e vogla.
  - Authentication AAA Authentication Server - Kjo metodë vërteton kundër një server qendror AAA që përmban emrat e përdoruesve dhe fjalëkalimet për të gjithë përdoruesit. Autentifikimi AAA i bazuar në server është i përshtatshëm për rrjetet mes të mëdha dhe të mëdha.
- Procesi për të dyja llojet shfaqet në rrëshqitjen tjetër.

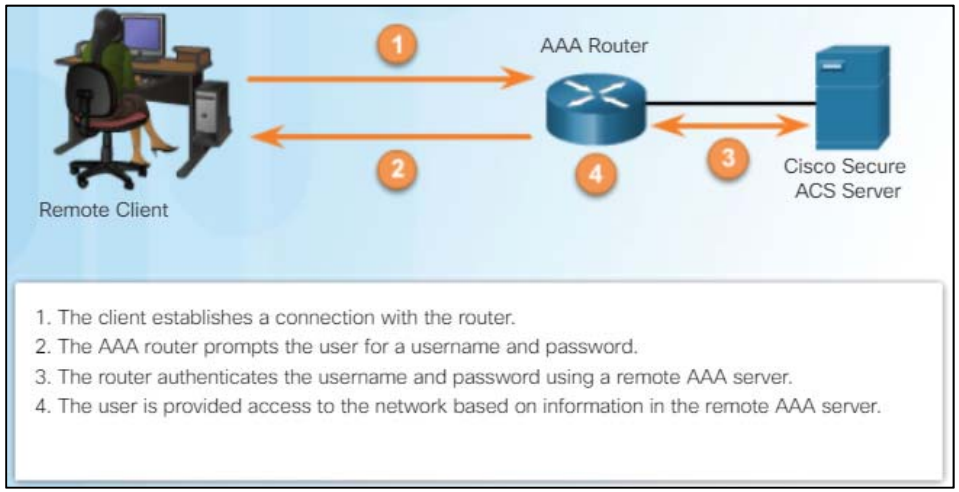
Përdorimi i AAA

Local AAA Authentication



1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using the local database and the user is provided access to the network based on information in the local database.

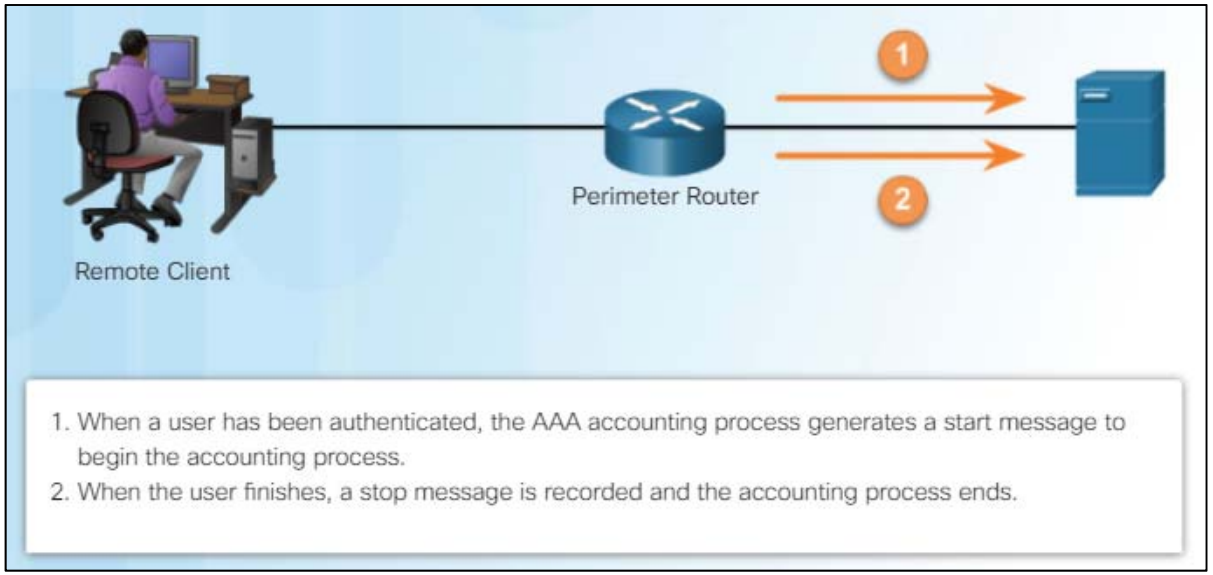
Server-Based AAA Authentication



1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a remote AAA server.
4. The user is provided access to the network based on information in the remote AAA server.

Përdorimi i AAA
AAA account registers

- Accounting siguron më shumë siguri sesa thjesht autentifikim.
- Serverat AAA mbajnë një regjistër të hollësishëm të saktësisht se çka bën përdoruesi i legalizuar në pajisje.



Përdorimi i AAA

AAA Accounting Logs (Cont.)

- Llojet e ndryshme të informacionit të kontabilitetit që mund të mblidhen përfshijnë:
  - Netowork Accounting- kap informacione të tilla si pikat e paketave dhe byte.
  - Connection Accounting - kap informacione për të gjitha lidhjet e jashtme.
  - EXEC Accounting - kap informacion rreth predhave të përdoruesit duke përfshirë emrin e përdoruesit, datën, kohën e fillimit dhe të ndalimit dhe adresën IP të serverit të qasjes.
  - System Accounting - kap informacione për të gjitha ngjarjet në nivel sistemi.
  - Command Accounting - kap informacion rreth komandave të ekzekutuara shell.
  - Resource Accounting - kap "mbështetje" e regjistrimit "start" dhe "stop" për thirrjet që kanë kaluar tek autentifikimi i përdoruesit.